AM 106/206: Applied Algebra **Prof. Salil Vadhan**

Problem Set 10

Assigned: Wed. Dec. 1, 2010 Due: Fri. Dec. 10, 2010 (2:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS10-yourlastname`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.
- Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (Density of Irreducible Polynomials) Let $F = \mathbb{F}_q$, and $E = \mathbb{F}_{q^n}$ for some prime power q.

1. Show that every element $a \in E$ is the zero of an irreducible polynomial in $F[x]$ of degree dividing n.
2. [AM106-A] Deduce that the number of monic irreducible polynomials in $F[x]$ of degree at most n is at least q^n/n, and the number of monic irreducible polynomials of degree exactly n is at least $q^n/n - q^{n/2}$.
3. [AM206-A] Prove that the number of monic irreducible polynomials in $F[x]$ of degree exactly n is at least $(q^n - 2q^{n/2})/n$. You may use the Möbius inversion formula, which says that if $f, g : \mathbb{N} \to \mathbb{R}$ satisfy $g(n) = \sum_{d|n} f(d)$ for all $n \geq 1$, then $f(n) = \sum_{d|n} \mu(d)g(n/d)$, where $\mu : \mathbb{N} \to \{-1, 0, 1\}$ is defined as follows:

$$\mu(d) = \begin{cases} 1 & \text{if } d \text{ square-free with an even number of prime factors} \\ -1 & \text{if } d \text{ square-free with an odd number of prime factors} \\ 0 & \text{if } d \text{ not square-free} \end{cases}$$

where a number d is *square free* if $d = p_1 p_2 \cdots p_k$ for distinct primes $p_1, \ldots, p_k$.

Problem 2. (Codes over Small Alphabets) The q-ary *Hadamard code* is the mapping $\mathrm{Had} : \mathbb{F}_q^k \to \mathbb{F}_q^{q^k}$ taking each $m \in \mathbb{F}_q^k$ to the tuple $(\langle m, v_1\rangle, \langle m, v_2\rangle, \ldots, \langle m, v_{q^k}\rangle)$, where $v_1, \ldots, v_{q^k}$ are a list of all elements of $\mathbb{F}_q^k$ and $\langle u, v\rangle = \sum_i u_i v_i$. That is, we view m as describing a linear function from $\mathbb{F}_q^k \to \mathbb{F}_q$ and the codeword is the evaluation of this linear function at all points. This code has very poor relative rate (k/q^k), but it has very good distance (as you will show) and can use very small alphabet sizes (even $q = 2$).

1. Show that the relative minimum distance of Had is $1 - 1/q$.
2. Combine a Reed-Solomon code over $\mathbb{F}_{2^\ell}$ for some ℓ and a Hadamard code to construct, for every $k = 2^\ell \geq 4$, an error-correcting code $\mathrm{Enc} : \{0,1\}^k \to \{0,1\}^{k^2}$ with relative minimum distance at least $1/4$. (Hint: view elements of $\{0,1\}^k$ as elements of $(\mathbb{F}_{2^\ell})^{\lceil k/\ell \rceil}$, encode these in a Reed-Solomon code, and then encode each resulting symbol in a Hadamard code.)

The above code has much better rate ($1/k$) than the Hadamard code, but still not constant. Nevertheless, this same approach of combining two codes ("code concatenation") is very widely used, and has been used to construct codes in which the rate, distance, and alphabet size are all constants independent of the message length k.

Problem 3. (Improved Decoding of Reed–Solomon Codes) Show that there is a polynomial-time algorithm for Noisy Polynomial Interpolation (see Lecture Notes 22) that works whenever the number s of agreements is larger than $\sqrt{2dn}$, improving the $2\sqrt{dn}$ bound from lecture. You may ignore round-off issues in your solution, and treat quantities like $\sqrt{2n/d}$ as integers. (Hint: do not use fixed upper bounds on the individual degrees in x and y of the interpolating polynomial $Q(x, y)$, but rather allow as many monomials as possible for Step 2 to go through.)